# 配置SD-WAN高級惡意軟體防護(AMP)整合和故 障排除

目錄
<u>必要條件</u>
採用元件
解決方案概述
<u>元件</u>
<u>功能流</u>
<u>SD-WAN AMP整合配置</u>
從vManage配置安全策略
<u>疑難排解</u>
<u>常規故障排除流程</u>
vManage上的策略推送問題
思科邊緣路由器上的AMP整合
<u>檢查UTD容器運行狀況</u>

# 簡介

本檔案介紹如何在Cisco IOS® XE SD-WAN路由器上設定和疑難排解Cisco SD-WAN進階惡意軟體 防護(AMP)整合。

# 必要條件

### 需求

思科建議您瞭解以下主題:

- 進階惡意軟體防護 (AMP)
- 思科軟體定義廣域網路(SD-WAN)

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設) )的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

# 解決方案概述

元件

SD-WAN AMP整合是SD-WAN邊緣安全解決方案的組成部分,旨在幫助分支機構使用者抵禦惡意軟 體。

它包括以下產品元件:

- 分支機構的WAN邊緣路由器。這是控制器模式下的Cisco IOS® XE路由器,其安全功能位於 UTD容器中
- AMP雲。AMP雲基礎設施以處置方式響應檔案雜湊查詢
- ThreatGrid。可在沙盒環境中測試檔案是否存在潛在惡意軟體的雲基礎架構

這些元件協同工作,為AMP提供以下主要功能:

• 檔案信譽評估

SHA256雜湊的過程,用於將檔案與高級惡意軟體防護(AMP)雲伺服器進行比較,並訪問其威脅情報 資訊。響應可以是Clean、Unknown或Malicious。如果響應為Unknown,且已配置File Analysis,則自動提交該檔案以進行進一步分析。

• 檔案分析

將未知檔案提交到ThreatGrid(TG)雲以在沙盒環境中進行爆轟。在引爆期間,沙盒捕獲偽像並觀察 檔案的行為,然後給出檔案的總得分。根據觀察結果和得分,Threat Grid可以將威脅響應更改為「 乾淨」或「惡意」。ThreatGrid的發現結果會報告給AMP雲,以便所有AMP使用者都能夠抵禦新發 現的惡意軟體。

追溯

它維護有關檔案的資訊,即使檔案下載後,我們也可以報告被下載後確定為惡意的檔案。檔案的處 置可能根據AMP雲獲得的新威脅情報而變化。此重新分類將生成自動追溯通知。

目前,整合了AMP的SD-WAN支援針對以下協定的檔案檢查:

- HTTP
- SMTP
- IMAP
- POP3
- FTP
- SMB

≫ 注意:僅支援<u>SSL</u>/TLS代理通過HTTPS<u>傳輸檔案</u>。

注意:檔案分析只能對完整的檔案執行,而不能對拆分為部分內容的檔案執行。例如,當 HTTP客戶端請求帶有Range標頭的部分內容並返回HTTP/1.1 206 Partial Content時。在這種 情況下,由於部分檔案雜湊與完整檔案有很大不同,Snort會跳過部分內容的檔案檢查。 功能流

該圖描述了當檔案需要提交到ThreatGrid進行分析時,SD-WAN AMP整合的高級流程。



對於顯示的流:

- 1. UTD容器會擷取AMP支援的通訊協定的檔案傳輸。
- 2. 計算檔案的SHA256雜湊。
- 3. 根據UTD中的本地快取系統查詢計算的SHA256雜湊,以檢視處置情況是否已知以及快取 TTL是否未過期。
- 4. 如果沒有與本地快取匹配的項,則會根據AMP雲查詢SHA256雜湊值,以確定處置和返回操作 。
- 5. 如果處置情況為UNKNOWN且響應操作為ACTION\_SEND,則檔案將通過UTD中的預分類系統運行。
- 6. 預分類器確定檔案型別, 並驗證檔案是否包含活動內容。
- 7. 如果同時滿足這兩個條件,則檔案將提交到ThreatGrid。
- 8. ThreatGrid會在沙盒中引爆檔案,並為檔案分配威脅評分。
- 9. ThreatGrid根據威脅評估更新AMP雲。
- 10. 邊緣裝置根據30分鐘的心跳間隔查詢AMP雲以進行回溯。

# SD-WAN AMP整合配置

✤ 注意:在配置AMP功能之前,必須將安全虛擬映像上傳到vManage。有關詳細資訊,請導航 到<u>安全虛擬映像</u>。

# ✤ 注意:檢視本文檔瞭解AMP/ThreatGrid連線正常工作的網路要求:<u>AMP/TG所需的IP地址/主</u> 機

# 從vManage配置安全策略

o

要啟用AMP,請導航至Configuration -> Security -> Add Security Policy。 選擇Direct Internet Access(直接訪問Internet),然後選擇Proceed(繼續),如下圖所示。

Add Security	y Policy	<
Choose a se	cenario that fits your use-case. Click Proceed to continue building your desired policies.	
=~	Compliance Application Firewall   Intrusion Prevention   TLS/SSL Decryption	
	Guest Access Application Firewall   URL Filtering   TLS/SSL Decryption	
	Direct Cloud Access Application Firewall   Intrusion Prevention   Advanced Malware Protection   DNS Security   TLS/SSL Decryption	
	Direct Internet Access Application Firewall   Intrusion Prevention   URL Filtering Advanced Malware Protection DNS Security   TLS/SSL Decryption	
٩,	Custom Build your ala carte policy by combining a variety of security policy blocks	
	Proceed Cancel	

### 根據需要配置安全功能,直至其進入「高級惡意軟體防護」功能。新增新的高級惡意軟體防護策略

≡	cisco vManage				٠	Ê	<b>#</b> ®	0	admin 🔻
5	CONFIGURATION Security > Add Security Policy								
▫	S Firewall S Intrusion Prevention	n 🥥 URL Filtering 🥥 Advanced Mahware Prot	DNS Security -	TLS/SSL Decryption		Policy Su			
٠									
٩									
÷									
**									
		<b>I</b>							
		Activate File Reputation and File Analysis to es	calate malware protection.						
		Create New Copy from Existing	stion Policy •						

提供策略名稱。選擇一個全域性AMP雲區域並啟用檔案分析。 對於使用ThreatGrid的檔案分析,選 擇其中一個TG雲區域,然後輸入可從ThreatGrid門戶的My ThreatGrid帳戶下獲取的ThreatGrid API金鑰。

≡	cisco vManage			•	自	#®	0	admin 👻
55		dd Advanced Malware Protection						
□ ≎		Target	Policy Behavior					
۹ ۹			AMP Cloud Region: NAM — TG Cloud Region: NAM — Reputation Alert Level: File Types List: 11 — Analysis Alert Level:	Critical Critical				
<u></u>		Contract MONA	File Reputation File Analysis Alerts					
•			Manage Threat Grid API Key X					
	Advanced Malware Prot	tection - Policy Rule Configuration	Select Region					
	AMP Cloud Region	NAM	NAM    Enter Key  Add					
	Alerts Log Level	Critical	EUR 🗡 🗑					
	File Analysis		Save Changes Cancel					
	TG Cloud Region	NAM	Threat Grid API Key: A Not Configured Manage API Key					
	File Types List							
	Alerts Log Level	Critical						

完成後,儲存策略,並在Additional Templates -> Security Policy下將此安全策略新增到裝置模板 ,如下圖所示。

≡	cisco vManage						٠	Û	<b>*</b> @	0	admin 🔻
8	CONFIGURATION   TEMPLAT	ES									
	<b>Basic Information</b>	Transport & Management VPN	Service	VPN	Additional Templates						
-		······································			Templete Name						
*	27fb5ff6-60ef-438f-91b8	8-a7e5ee586a58			CSR1kv_SDWAN-lab-CSR1k-service-vpn1-DIA Cisco VF	VPN Interface Ethernet					
3											
÷	Additional Templates										
<b></b>	Additional remplates										
	AppQoE	Choose	٠								
	Global Template *	Factory_Default_Global_CISCO_Template	•	0							
	Cisco Banner	Choose	•								
	Cisco SNMP	Choose	•								
	CLI Add-On Template	Choose	•								
	Policy	Chappe	-								
		unouse									
	Probes	Choose	•		_						
	Security Policy	DIA-Security-Policy	•								
	Container Profile *	Factory_Default_UTD_Template		0	-						
					Update Cancel						

使用更新的裝置模板配置裝置。

驗證

成功將裝置模板推送到邊緣裝置後,可以從邊緣路由器CLI驗證AMP配置:

#### <#root>

```
branch1-edge1#show sdwan running-config | section utd
app-hosting appid utd
app-resource package-profile cloud-low
app-vnic gateway0 virtualportgroup 0 guest-interface 0
 guest-ipaddress 192.168.1.2 netmask 255.255.255.252
!
app-vnic gateway1 virtualportgroup 1 guest-interface 1
 guest-ipaddress 192.0.2.2 netmask 255.255.255.252
!
start
utd multi-tenancy
utd engine standard multi-tenancy
threat-inspection profile IPS_Policy_copy
threat detection
policy balanced
logging level notice
I
utd global
file-reputation
 cloud-server cloud-isr-asn.amp.cisco.com
 est-server cloud-isr-est.amp.cisco.com
I
file-analysis
cloud-server isr.api.threatgrid.com
apikey 0 <redacted>
!
1
file-analysis profile AMP-Policy-fa-profile
file-types
 pdf
 ms-exe
 new-office
 rtf
 mdb
 mscab
 msole2
 wri
 xlw
 f1v
 swf
!
alert level critical
ļ
file-reputation profile AMP-Policy-fr-profile
alert level critical
!
file-inspection profile AMP-Policy-fi-profile
```

analysis profile AMP-Policy-fa-profile

```
reputation profile AMP-Policy-fr-profile
```

```
!
policy utd-policy-vrf-1
all-interfaces
```

file-inspection profile AMP-Policy-fi-profile

```
vrf 1
threat-inspection profile IPS_Policy_copy
exit
policy utd-policy-vrf-global
all-interfaces
```

file-inspection profile AMP-Policy-fi-profile

```
vrf global
exit
no shutdown
```

### 疑難排解

SD-WAN AMP整合涉及多個元件,如所述。因此,進行故障排除時,必須建立一些關鍵分界點,將 問題縮小到功能流中的元件:

- 1. vManage.vManage是否可以成功將具有AMP策略的安全策略推送到邊緣裝置?
- 2. 邊緣。安全策略成功推送到邊緣後,路由器是否捕獲要接受AMP檢查的檔案並將其傳送到 AMP/TG雲?
- AMP/TG雲。如果邊緣將檔案傳送到AMP或TG,它是否獲得做出允許或丟棄決策所需的響應
   ?

本文將側重於邊緣裝置(2),以及各種資料平面工具,幫助排除WAN邊緣路由器上的AMP整合問題 。

常規故障排除流程

使用此高級工作流程快速排除AMP整合涉及的各種元件的故障,關鍵目標是建立邊緣裝置與 AMP/TG雲之間的問題分界點。

- 1. AMP策略是否正確推送到邊緣裝置?
- 2. 檢查UTD容器的一般運行狀況。
- 3. 檢查檔案信譽並分析邊緣上的客戶端狀態。
- 4. 檢查檔案傳輸是否轉移到容器。可以使用Cisco IOS® XE資料包跟蹤來完成此操作。
- 5. 檢查以確認邊緣已成功與AMP/TG雲通訊。可以使用EPC或資料包跟蹤等工具完成此操作。
- 6. 確保UTD根據AMP響應建立本地快取。

本檔案將詳細探討這些疑難排解步驟。

vManage上的策略推送問題

如AMP策略配置所示,AMP策略非常簡單,沒有很多配置選項。以下是需要考慮的一些常見問題:

- 1. vManage必須能夠解析AMP的DNS名稱以及用於API訪問的ThreatGrid雲。如果新增AMP策略 後,vManage上的裝置配置失敗,請檢視/var/log/nms/vmanage-server.log中是否有錯誤。
- 2. 如配置指南中所述,「警報日誌級別」已保留預設嚴重級別,或者「警告」(如果保證)。必須避免資訊級記錄,因為它可能會對效能產生負面影響。

要驗證,請訪問neo4j DB並檢視vmanagedbAPIKEYNODE表的內容。

neo4j@neo4j> match (n:vmanagedbAPIKEYNODE) return n; +
+   n   +
+   (:vmanagedbAPIKEYNODE {_rid:
"0:ApiKeyNode:1621022413389:153", keyServerHostName: "isr.api.threatgrid.com", feature: "Amp", apiKey:
$\label{eq:crypt_clusters} \end{tabular} \label{eq:crypt_clusters} where \end{tabular} \end{tabular} \label{eq:crypt_clusters} \end{tabular} \end{tabular} where \end{tabular} tab$
07B6865F-7FE7-BA0D-7240-1BDA16328455"})   +
+

### 思科邊緣路由器上的AMP整合

### 檢查UTD容器運行狀況

使用show utd命令檢查UTD容器的整體運行狀況:

show utd engine standard config show utd engine standard status show platform hardware qfp active feature utd config show platform hardware qfp active feature utd stats show app-hosting detail appid utd show sdwan virtual-application utd

檢查UTD AMP狀態

#### 確保已啟用檔案檢查:

#### <#root>

branch1-edge1#show sdwan utd dataplane config utd-dp config context 0 context-flag 25427969 engine Standard state enabled sn-redirect fail-open redirect-type divert threat-inspection not-enabled defense-mode not-enabled domain-filtering not-enabled url-filtering not-enabled all-interface enabled

file-inspection enabled

utd-dp config context 1 context-flag 25559041 engine Standard state enabled sn-redirect fail-open redirect-type divert threat-inspection enabled defense-mode IDS domain-filtering not-enabled url-filtering not-enabled all-interface enabled

file-inspection enabled

#### 驗證與AMP雲的連線是否已啟動:

#### <#root>

branch1-edge1#show utd engine standard status file-reputation File Reputation Status: Process:

#### Running

Last known status: 2021-06-17 16:14:20.357884-0400 [info] AMP module version 1.12.4.999

#### <#root>

branch1-edge1#show sdwan utd file reputation utd-oper-data utd-file-reputation-status version 1.12.4.999

utd-oper-data utd-file-reputation-status status utd-file-repu-stat-connected

utd-oper-data utd-file-reputation-status message "Connected to AMP Cloud!"

驗證與ThreatGrid的連線是否已啟動:

<#root>

branch1-edge1#show utd engine standard status file-analysis File Analysis Status: Process:

#### Running

Last Upload Status: No upload since process init

#### <#root>

branch1-edge1#show sdwan utd file analysis

utd-oper-data utd-file-analysis-status status tg-client-stat-up

```
utd-oper-data utd-file-analysis-status backoff-interval 0
utd-oper-data utd-file-analysis-status message "TG Process Up"
```

如果ThreatGrid進程未顯示Up狀態,則API重新生成金鑰會有所幫助。要觸發API重新生成金鑰,請 導航到Maintenance -> Security:

≡	diada cisco	Cisco vManage					
::	🖆 MAI	INTENANCE   SECURITY					
	Applic	ation Firewall Intrusion Prevent	ion URL Filtering Advanced	Malware Protection Umbrella	DNS Security		
۵	1 Row	vs Selected Action -					
a	Device	Group All API Rekey		Search Options 🗸			
`		Hostname	System IP	Chassis Number	Device Model	Virtual Image State	Virtual Image Version
÷		😢 branch1-cedge1	6.1.1.11	CSR-07B6865F-7FE7-BA0D-7240	CSR1000v	RUNNING	1.0.6_SV2.9.13.0_XE17.3
*							
12							

💊 注意:API重新生成金鑰會觸發向裝置的模板推送。

# WAN邊緣路由器上的AMP活動監控

vManage

通過vManage,可以從安全控制面板或裝置檢視監控AMP檔案活動。

安全儀表板:



### 裝置檢視:

	ge					•	i 🕯 🗚	9	ac
	rk > Advanced Malware Protection								
Select Device •	branch1-cedge1   6.1.1.11 Site ID: 100	Device Model: CSR1000v 0							
TCP Optimization	File Reputation								
WAN Throughput			<u>~</u> 🗘						
Flows	50							1	
Top Talkers								A	
WAN	40							-	
								- 11	
ILDC	<u>2</u> 30							- 11	
Tunnel	a log								
Security Monitoring	ag En 20								-
Firewall									
Intrusion Prevention	10								
Intrusion Prevention	10								-
Intrusion Prevention URL Filtering Advanced Malware	10 0 • • • • • • • • • • • • • • • • • •	00 Jun 20, 20.00 Jun 21, 00.00 Jun 21, 00.00 Jun 20	1,02:00 Jun 21,04:00	Jun 21, 06:00 Jun 21, 08:00	Jun 21, 10:00	Jun 21, 12:00	Jun 21, 14:00	Jun 21, 16	6:00
Intrusion Prevention URL Filtering Advanced Malware Protection	10 0 •••• • • • • • • • • • • • • • • • •	00 Jun 20, 20,00 Jun 20, 22,00 Jun 21, 00,00 Jun 2	1, 02:00 Jun 21, 04:00 J	yun 21, 06:00 Jun 21, 08:00	Jun 21, 10:00	Jun 21, 12:00	Jun 21, 14:00	Jun 21, 10	6:00
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption	10	00 jun 20, 20,00 jun 20, 22:00 jun 21,00:00 jun 2	1,02:00 Jun 21,04:00 J	Jun 21, 06:00 Jun 21, 08:00	Jun 21, 10:00	Jun 21, 12:00	Jun 21, 14:00	Jun 21, 10	6:00
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption Umbrelia DNS Re-	10 0 •••••••••••••••••••••••••••••••••••	00 jun 20, 20,00 jun 20, 22:00 jun 21,00:00 jun 2 Search Options ↓	, 02:00 Jun 21, 04:00 J	Jun 21, 06:00 Jun 21, 08:00	Jun 21, 10:00	Jun 21, 12:00	Jun 21, 14:00	Jun 21, 16	6:00 () () () () () () () () () () () () ()
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption Umbrella DNS Re- direct	10 0 •••••••••••••••••••••••••••••••••••	00 jun 20, 20,00 jun 20, 22:00 jun 21,00:00 jun 2 Search Options ↓	1, 02:00 jun 21, 04:00 j	Jun 21, 06:00 Jun 21, 08:00	Jun 21, 10:00	Jun 21, 12:00	Jun 21, 14:00	Jun 21, 16	6:00 () () () () () () () () () () () () ()
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption Umbrelia DNS Re- direct Control Connections	10 0 •••••••••••••••••••••••••••••••••••	00 jun 20, 20.00 jun 20, 22.00 jun 21, 00.00 jun 2 Search Options ✓ SHA-256(Hash) 788908c1ddac169a6c147a781c3b1b7ec637797e88b0f42a6a5t	1, 02:00 Jun 21, 04:00 J File Type Di L PNG Ur	Jun 21, 06:00 Jun 21, 08:00 Isposition Time nknown 21 Jun 202	Jun 21, 10:00	Jun 21, 12:00 VPN 1	Jun 21, 14.00 Action Allow	Jun 21, 10	6:00 (5:49
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption Umbrella DNS Re- direct Control Connections Sector Status	10 0 •••••• jun 20, 18 Q File Name sand png putty_unknown.exe	00 Jun 20, 20:00 Jun 20, 22:00 Jun 21, 00:00 Jun 2 Search Options ✓ SHA-256(Hash) 788908c1ddac169a6e147a781e3b1b7ec637797e88b0l42a6a51 833a609ca00665ebb4ec10be2/fc115b4d48c2e02c02b73906d71	File Type         Ot           File Type         Ot           msEXE         Ur	Jun 21, 06:00 Jun 21, 08:00 sposition Time nknown 21 Jun 20 sknown 21 Jun 202	Jun 21, 10:00	Jun 21, 12:00 VPN 1 1	Jun 21, 14:00 Action Allow Allow	Jun 21, 10	6:00 es: 49
Intrusion Prevention URL Filtering Advanced Malwere Protection TLS/SSL Decryption Umbrelia DNS Re- direct Control Connections System Status	10 0 ••••• jun 20, 18: Q File Name sand png putty_unknown.exe putty.exe	00 Jun 20, 20.00 Jun 20, 22.00 Jun 21, 00.00 Jun 2 Search Options ✓ SHA-256(Hash) 78a/908c1ddac169a6e147a781e3b1b7ec637797e88b0f42a6a51 833a609ca00665eb04ec10be2/c115b4d48c2e02c02b73906d7N 13d8429d500e20be85881250449f70a6e818f34df9423b2897fd3	File Type         Ol           Image: Second Seco	Jun 21, 06:00 Jun 21, 08:00  sposition Time nknown 21 Jun 20 nknown 21 Jun 202 nknown 21 Jun 202	Jun 21, 10:00 1 4:22:01 PM EDT 1 4:21:51 PM EDT 1 4:21:43 PM EDT	Jun 21, 12:00 VPN 1 1 1	Jun 21, 14:00 Action Allow Allow Allow	Jun 21, 10	6:00 es: 49
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption Umbrella DNS Re- direct Control Connections System Status Events	10 0 •••• Jun 20, 18: Q File Name sand png putty_unknown.exe putty exe makemalware.exe	00 Jun 20, 20.00 Jun 20, 22.00 Jun 21, 00.00 Jun 2 Search Options ✓ 584A-256(Hash) 78a908c1ddac169a6c147a781e3b1b7ec637797e88b0l42a6a51 833a609ca00665ebb4ec10be2/c115b4d48c2e02c02b73906d74 1348429d50be20be85881250449f70a6e818f34df9423b2897fd3 aeba9139fe18d27e40d0629d80ba3b2eeea003fb5b33a376c611	File Type         Di	Jun 21, 06:00 Jun 21, 08:00 isposition Time nknown 21 Jun 202 nknown 21 Jun 202 nknown 21 Jun 202 lalicious 21 Jun 202	Jun 21, 10:00 1 422:01 PM EDT 1 421:51 PM EDT 1 421:43 PM EDT 1 421:38 PM EDT	Jun 21, 12:00 VPN 1 1 1 1 1	Jun 21, 14:00 Action Allow Allow Allow Drop	Jun 21, 10	6:00 es: 49
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SEL Decryption Umbrella DNS Re- direct Control Connections System Status Events ACL Logs	10 0 ••••• jun 20, 18: Q File Name sand png putty_unknown.exe putty exe makemalware.exe eicar.com.txt	00 Jun 20, 20.00 Jun 20, 22.00 Jun 21, 00.00 Jun 2 Search Options V SHA-256(Hash) 78a908c1ddac169a6c147a781c3b1b7cc537797c88b0l42a6a51 833a609ca00665ebb4ec10ba2fc115b4d48c2e02c02b73906d7 13d8429d500e20be85881250449f70a6e818f34df9422b2897fd3 aeba9f39fc18d27c400d0c59d80ba3b2eeea003fb5b33a376c611 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538	File Type         D           File Type         D           with the type         D            PNG         Ur            MSEXE         Ur            MSEXE         Ur            MSEXE         MSEXE	Jun 21, 06:00 Jun 21, 08:00 isposition Time Aknown 21 Jun 202 nknown 21 Jun 202 nknown 21 Jun 202 lalicious 21 Jun 202 allicious 21 Jun 202	Jun 21, 10:00 1 422:01 PM EDT 1 421:51 PM EDT 1 421:43 PM EDT 1 421:38 PM EDT 1 421:34 PM EDT	ypn 21, 12:00 VPN 1 1 1 1 1 1 1 1	Jun 21, 14:00 Action Allow Allow Drop Drop	Jun 21, 10	6:00 () () () () () () () () () () () () ()
Intrusion Prevention URL Filtering TLS/SSL Decryption Umbrelia DNS Re- direct Control Connections System Status Events ACL Logs	10 0 •••••••••••••••••••••••••••••••••••	00 Jun 20, 20.00 Jun 20, 22:00 Jun 21, 00.00 Jun 2 Search Options ↓ 584A-256(Hash) 78a908c1ddac169a6e147a781e3b1b7ec637797e88b0f42a6a5f 833a69ca00655ebb4ec10be2fc115b4d48c2e02c02b73906d7/ 13d8429d500e20be85881250449f70a6e818f34df9422bc2897fd3 aeba9f39fe18d27e40d0629d80ba3b2eeea003fb5b33a376c611 275a021bbfb6489e54d471699f7db9d1663fc695ec2fe2a2c4533 5cbf56e3c3b07259f648932bc4c39a2103ef1a0946139ac2721b	File Type         Dt           File Type         Dt           PNG         Ut           MSEXE         Ut           DDF         Ut	Jun 21, 06:00 Jun 21, 08:00 Isposition Time Inknown 21 Jun 202 Inknown 21 Jun 202 Inknown 21 Jun 202 Ialicious 21 Jun 202 Ialicious 21 Jun 202 Ialicious 21 Jun 202	Jun 21, 10:00 1 422:01 PM EDT 1 421:51 PM EDT 1 421:32 PM EDT 1 421:38 PM EDT 1 421:34 PM EDT 1 421:30 PM EDT	Jun 21, 12:00	Jun 21, 14.00 Action Allow Allow Drop Drop Drop	Jun 21, 14	6:00 () () () () () () () () () () () () ()
Intrusion Prevention URL Filtering Advanced Malware Protection TLS/SSL Decryption Umbrelia DNS Re- direct Control Connections System Status Events ACL Logs Troubleshooting	10 0 Jun 20, 18: Q File Name sand png putty_unhown.exe putty exe makemalware.exe eicar.com.tut document1.pdf sand.png	00 jun 20, 20,00 jun 20, 22,00 jun 21,00,00 jun 2 Search Options ✓ SHA-256(Hash) 78a908c1ddac169a6e147a781c3b1b7ec637797e88b0/42a6a58 13a6429d500e20be85881250449f70a6e816134df9422b2897Hd3 aeba91391618427e40d0629480ba3b2ceeaa003fb83b3a376c611 275a021bbb6489e54d4718997fd9hd16a3i62695ec27e12a2aC433 5cbf56e3c3b07259648932bc4c39a2103ef1a0a946139ac2f21b 78a908c1ddac169a6e147a781c3b1b7ec637797e88b0/42a6a58	File Type         DV           File Type         DV           m Sexe         Ur            MSEXE         Ur            POF         Ur            PDF         Ur	Jun 21, 06:00 Jun 21, 08:00 isposition Z1 Jun 20 nknown 21 Jun 202 nknown 21 Jun 202 allicious 21 Jun 202 allicious 21 Jun 202 nknown 21 Jun 202 nknown 21 Jun 202	1 422.01 PM EDT 1 421.51 PM EDT 1 421.51 PM EDT 1 421.43 PM EDT 1 421.38 PM EDT 1 421.30 PM EDT 1 421.30 PM EDT 1 421.30 PM EDT	Jun 21, 12:00 VPN 1 1 1 1 1 1 1 1	Jun 21, 14.00 Action Allow Allow Drop Drop Drop Allow Allow	Jun 21, 11	6:00

### CLI

### 檢查檔案信譽統計資訊:

branch File R 	1-edge1#sh eputation	ow utd engine Statistics	standard	statistics	file-reputation
File R	eputation	Clean Count:		1	
File R	eputation	Malicious Coun	t:	4	
File R	eputation	Unknown Count:		44	
File R	eputation	Requests Error	:	0	
File R	eputation	File Block:		4	
File R	eputation	File Log:		45	

branch1-edge1#show utd engine standard statistics file-analysis
File Analysis Statistics
----File Analysis Request Received: 2
File Analysis Success Submissions: 2
File Analysis File Not Interesting: 0
File Analysis File Whitelisted: 0

File Analysis File Not Supported:0File Analysis Limit Exceeding:0File Analysis Failed Submissions:0File Analysis System Errors:0

注意:可以使用show utd engine standard statistics file-reputation vrf global internal命令獲取其他 內部統計資訊。

#### 資料平面行為

根據配置的AMP策略進行檔案檢查的資料平面流量將轉移到UTD容器進行處理。這可以通過使用資料包跟蹤進行確認。如果流量沒有正確轉移至容器,則不會執行任何後續的檔案檢查操作。

#### AMP本地檔案快取

UTD容器具有SHA256雜湊、檔案型別、處置以及基於先前AMP雲查詢結果的操作的本地快取。如 果檔案雜湊不在本地快取中,則容器僅從AMP雲請求處置。在刪除快取之前,本地快取的TTL為2小 時。

branch1-edge1#show utd engine standard cache file-inspection Total number of cache entries: 6 File Name| File Type| Disposition| action| SHA256 \_\_\_\_\_ sand.png putty.exe 78A908C1DDAC169A 69 1 1 putty.exe13D8429D500E20BEmakemalware.exeAEBA9F39FE18D27Eputty\_unknown.exe833A609CA00665EBdocument1.pdf5CBF56E3C3B07259eicar.com.txt275A021BBFB6489E 21 1 2 21 3 2 21 2 1 285 1 1 273 3 2

#### AMP處置代碼:

0 NONE

1 UNKNOWN

2 CLEAN

3 MALICIOUS

### AMP操作代碼:

0 UNKNOWN

1 ALLOW

2 DROP

若要取得檔案的完整SHA256雜湊值(這對解決特定檔案判定問題非常重要),請使用命令的 detail選項:

branch1-edge1#show utd engine standard cache file-inspection detail SHA256: 78A908C1DDAC169A6E147A781E3B1B7EC637797E88B0F42A6A5B59810B8E7EE5 amp verdict: unknown amp action: 1 amp disposition: 1 reputation score: 0 retrospective disposition: 0 amp malware name: file verdict: 1 TG status: 0 file name: sand.png filetype: 69 create\_ts: 2021-06-21 16:58:1624309104 sig\_state: 3 \_\_\_\_\_ SHA256: 13D8429D500E20BE8588F250449F70A6E8F8F34DF9423B2897FD33BBB8712C5F amp verdict: unknown amp action: 2 amp disposition: 1 reputation score: 0 retrospective disposition: 0 amp malware name: file verdict: 1 TG status: 7 file name: putty.exe filetype: 21 create\_ts: 2021-06-21 16:58:1624309107 sig\_state: 3 \_\_\_\_\_ SHA256: AEBA9F39FE18D27E40D0629D80BA3B2EEEA003FB5B33A376C611BB4D8FFD03A6 amp verdict: malicious amp action: 2 amp disposition: 3 reputation score: 95 retrospective disposition: 0 amp malware name: W32.AEBA9F39FE-95.SBX.TG file verdict: 1 TG status: 0 file name: makemalware.exe filetype: 21 create\_ts: 2021-06-21 16:58:1624309101 sig\_state: 3 <SNIP>

#### 若要刪除UTD引擎本地快取條目,請使用命令:

clear utd engine standard cache file-inspection

### 運行UTD調試

可以啟用utd調試來排除AMP故障:

debug utd engine standard file-reputation level info debug utd engine standard file-analysis level info debug utd engine standard climgr level info

可以直接從系統shell(位於/tmp/rp/trace/vman\_utd\_R0-0.bin)中檢索調試輸出,或者按以下步驟將跟 蹤檔案複製到路由器檔案系統:

branch1-edge1#app-hosting move appid utd log to bootflash: Successfully moved tracelog to bootflash:/iox\_utd\_R0-0\_R0-0.5113\_0.20210622110241.bin.gz branch1-edge1#

檢視UTD跟蹤日誌:

```
branch1-edge1#more /compressed bootflash:/iox_utd_R0-0_R0-0.5113_0.20210622110241.bin.gz
<snip>
2021-06-22 10:35:04.265:(#1):SPP-FILE-INSPECTION File signature query: sig_state = 3
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION start_time : 1624372489, current_time : 1624372504,Dif
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_node_exists:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Signature not found in cache
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION file_type_id = 21
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Write to cbuffer
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Sent signature lookup query to Beaker
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION File Name = /putty_unknown.exe, file_name = /putty_unk
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_extract_filename :: Extracted filename 'putty_unkn
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_add:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION amp_cache_allocate:: Entry
2021-06-22 10:35:04.266:(#1):SPP-FILE-INSPECTION Return FILE_VERDICT_PENDING
<SNIP>
```

💊 註:在20.6.1及更高版本中,檢索和檢視utd tracelogs的方式與使用show logging process vman module utd ...命令的標準跟蹤工作流一致。

### 驗證從邊緣到雲的通訊

要驗證邊緣裝置與AMP/TG雲通訊,WAN邊緣路由器上的EPC可用於確認與雲服務之間存在雙向通 訊:

branch1-edge1#show monitor capture amp parameter monitor capture amp interface GigabitEthernet1 BOTH monitor capture amp access-list amp-cloud monitor capture amp buffer size 10 monitor capture amp limit pps 1000

# AMP和TG雲相關問題

確認邊緣裝置正確捕獲檔案並將其傳送到AMP/TG進行分析,但判定不正確,則需要AMP故障排除 或Threatgrid雲,這超出了本文檔的範圍。在出現整合問題時,資訊非常重要:

- ThreatGrid帳戶組織
- 時間戳
- 裝置分析ID(例如,CSR-07B6865F-7FE7-BA0D-7240-1BDA16328455),這是WAN邊緣路由 器的機箱編號。
- 完成相關檔案的SHA256雜湊

# 相關資訊

- <u>SD-WAN安全配置指南</u>
- <u>ThreatGrid</u>門戶
- <u>技術支援與文件 Cisco Systems</u>

### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。